1

Method and System for Authenticating a User

Technical Field

5   This invention relates to a system and method for generating an authentication rating for
an entity. More particularly, but not exclusively, the invention relates to a distributed
authentication system which automatically generates an authentication rating for the entity
according to a set of predefined fuzzy inferencing rules.

10   Background to the Invention and Prior Art

The process of securing IT services is a complex and continuously evolving battle
between defensive and offensive strategies. An important aspect of this process is the
authorisation of legitimate users of IT resources, as it is the human element which is the
15   weakest link in any security architecture. Good encryption techniques and strong public-
key mechanisms assist in securing IT services, but if the end user of the system cannot
be authenticated as a valid user then the whole security strategy fails.

When compared with the level of technology commonly applied in the domains of intrusion
20   detection and firewall management (in which an extensive number of commercially
available software and hardware solutions exist), the domain of user authentication has
been significantly neglected. For a significant proportion of applications, a simple user
password login is all that is required for authentication. Developments in the area of
authentication include the use of biometric methods, such as fingerprint or iris-scan
25   identification, however the cost of these technologies is still prohibitive. Alternatively,
authentication may be carried out using smart cards with hardware encryption. This is a
very secure solution, which is widely used in military and sensitive commercial areas, but
is expensive and costly to manage. Also if the card is lost or stolen a serious security
breach can occur.
30
With the rapid expansion of electronic commerce, organisations are increasingly exposing
their internal infrastructure to wireless, web and other access mechanisms, and with it
their ability to protect that infrastructure with perimeter defence systems declines. A lack
of manpower within companies can lead to user-access rights not being properly tracked,
35   and limited oversight of system administrative changes. Web Services, an entire concept

which revolves around constant, secure data trading is a particular area concerned with authentication since ultimately employees, business partners, customers and suppliers will be talking to each other through such mechanisms.

5   In view of this, a number of authentication systems are being developed in which a plurality of sources are used for improved robustness during authentication. One example of this is described in **"Multimodal Decision-Level Fusion for Person Authentication" by Vassilios Chatzis, Adrian G. Bors, and Ioannis Pitas, IEEE Trans. on Systems, man and Cybernetics, Part A: Systems and Humans, pp.674-681, Nov. 1999**, in which
10   a fuzzy clustering algorithm is used to combine the output from face and voice recognition systems. This document describes a user authentication system which combines various different methods for authenticating a person, such as voice features and face image information including shape and grey-level values.

15   With regard to authenticating other software entities, a further document, **"An Evidential Model of Distributed Reputation Management" by Bin Yu and Munindar P. Singh, Int. Conf., Autonomous Multi-Agent Systems, Bologna, Italy, 2002,** deals with the issue of trust within a community of software agents. This document discusses the advantages of collaborative behaviour between agents to evaluate the trustworthiness of
20   each other, and proposes a Bayesian method for combining trust assessments from multiple agents. This paper is concerned with the issue of updating an agent's rating by obtaining testimonies from other agents, and in particular how to manage a chain of referrals until an appropriate agent is contacted who can give information on interactions it has had with the agent in question.
25
     Accordingly, it is an object of the present invention to seek to provide an improved authentication system and method for authenticating an entity (which could be, for example, a human entity, a software agent or Web service).

30   A first aspect of the present invention provides a method for generating an authentication rating for an entity, comprising:
     receiving a message identifying an entity, which message requires authentication of said entity;
     receiving data from each of a plurality of sources, said data representing at least a rating
35   for said authentication according to a criteria;

analysing said received data using a set of predefined fuzzy inferencing rules so as to calculate an authentication rating for said entity

A second aspect of the present invention provides a system for generating an
5   authentication rating for an entity, comprising:
        receiving means for receiving a message identifying an entity, which message requires identification of said entity;
        the receiving means being further arranged to receive in use from each of a plurality of sources data representing a rating of said entity according to a criteria; and
10   processing means arranged in use to analyse said received data using a set of predefined fuzzy inferencing rules so as to calculate an authentication rating for said entity.

For a better understanding of the present invention, specific embodiments will now be
15   described, by way of example, with reference to the accompanying drawings, in which:
        Figure 1 shows a computer network including an authentication server according to an embodiment of the invention;
        Figure 2 shows a schematic of the authentication server according to an embodiment of the invention;
20   Figure 3 is a flow chart illustrating an authentication process performed by the authentication server of Figure 2;
        Figure 4 illustrates fuzzy input sets for trust and confidence ratings;
        Figure 5 illustrates examples of assigning trust and confidence ratings to a set of fuzzy rules;
25   Figure 6 shows a representation of all possible fuzzy output sets for a set of fuzzy rules;
        Figure 7 shows a schematic of a multi-agent distributed authentication system according to a second embodiment of the invention;
        Figure 8 is a network diagram of the system of Figure 7; and
        Figure 9 shows a functional block diagram of the inputs to the inferencing component of
30   the embodiments of the invention.

        Figure 1 illustrates a computer network which includes an authentication server 1 according to an embodiment of the invention. In this example, the authentication server 1 forms part of an authentication web service 4, and is connected to a Web server 2
35   hosting, for example, a popular travel web site which is accessible to users via a Web

4

· browser interface 3. In a typical scenario, a user 5 wishing to purchase travel tickets via the Web site, logs on via browser interface 3. The user logs on using a single username and password, which is forwarded in an authentication request by the Web server 2 to the authentication web service 4. The authentication web service 4 then invokes its local
5 authentication server 1 to determine whether or not to authenticate the user.

The forwarding web site 2 has included with its authentication request an evaluation of the level of trust it assigns to the login information provided by the user 5. In this case two numerical variables are used: a trust rating to indicate the level of trust, and a confidence
10 rating for that trust level, and these have been assigned 0.9 and 0.2 respectively (out of a range of 0 to 1). The authentication web service 4 invokes its local authentication server 1 using a structured message format based on XML, and includes the trust and confidence ratings as *TrustValue* and *ConfidenceRating* respectively in the message. · Subsequent processing by the authentication server 1 is described with reference to Figures 2 and 3.

15
Figure 2 schematically illustrates authentication server 1. The XML message object 21 is received from the Web Service 4 via a pre-processing module 22. Referring to Figure 3, the arrival of the XML message object (step S3.1) initiates a new Authenticate Request Process. The XML message is filtered (step S3.2) to extract *TrustValue* and
20 *ConfidenceRating*. The authentication server 1 then communicates with a local database 7 (part of the authentication web service 4) which contains users' previous case data, so as to retrieve any relevant earlier case details for this user. In this case it is determined (step S3.4) that no previous case history exists for this user in the databse 7, and so the ·*TrustValue* and *ConfidenceRating* from the XML message object 21 are passed for
25 processing (step S3.5) to the fuzzy inferencing module 25. At step S3.6, an authentication rating is output from the fuzzy inferencing module, and compared against a predefined security policy (step S3.7) to determine if it meets a policy-determined threshold limit.

In this instance, the authentication rating does not reach the policy threshold, so
30 processing moves to step S3.8 to create a message object indicating that access should be denied, and this is returned to the calling service, ie the authentication web service 4. In this case, the web service policy determines on the basis of the response that a second set of reputation data is required for this user. The authentication service 4 sends an authenticate request to a Trusted Third Party (TTP) 6. The TTP responds, using the
35 structured XML message format, with data it holds relating to the authentication of the

user, including two further numeric data values corresponding to *TrustValue* and *ConfidenceRating*, and the web service creates a new authenticate request object which it passes to the authentication server 1 including *TrustValue* and *ConfidenceRating*. Processing again moves through the flow chart of Figure 3 as before, with this time step

5   S3.4 determining that case data for this user (stored as a result of the previous pass through the processing) is now stored in the database. At step S3.12, this previous case data is retrieved and passed on (step S3.13) for processing by the fuzzy rule sytem. This time, the previous ratings are combined (step 3.5) new trust and confidence ratings and a revised authentication rating is output. The output authentication rating now satisfies the

10   security policy threshold (step S3.7), and so processing moves to step S3.10 where the data-formatting module 26 creates an authenticate signal (again in the form of an XML message object 27) which is sent in step S3.11 back to the calling service (ie the authentication web service 4). The authentication web service 4 then communicates with the calling web server 2, indicating that it should grant access to the user.

15

With reference to Figure 2, the input/output channels to the fuzzy inferencing module 25 via the preprocessing module 22 and formatting module 26 can be seen. This arrangement allows a generic authenticate object to be passed from the calling service via the pre-processing class to the Inferencing component, and for a new authenticate

20   response object to be generated and passed back to the calling service. These pre and post processing classes allow dynamic reconfiguration of the data format based on current policy requirements, and hence no run-time modifications to the Inferencing component will normally be required. The database access occurs external to the Inferencing process within a class for parsing structured data from the message objects.

25

The authentication server 1 further includes a policy manager 23 which stores policy requirements and a module 28 for generating updated version of fuzzy rules. The policy manager 23 is configurable by a system administrator, and determines on the basis of the authentication ratings whether the user's authentication request should be granted or

30   rejected.

As already mentioned, after a case has been evaluated, the authentication result is stored in the local user case database 7 by the system, including the date and timestamp of the transaction. When the same user makes a request at any future date this information is

35   retrieved from the database and combined with the current trust ratings to generate a new

6

evaluation. Specifically, the length of time a user has been known to the system can form one input to a fuzzy rule which allocates an increased level of trust proportional to the length of time a user has been known to the system (presuming no violation by that user of any resource has been recorded by the system).

5

With reference to Figures 4, 5 and 6, the fuzzy based inferencing performed by the fuzzy inferencing module 25 will now be described in more detail. The theoretical basis behind the inferencing is that soft computing techniques can be successfully applied to generate an authentication rating for an entity (eg a human user, software agent or web service)

10   based on a plurality of varied inputs. This is a two-stage process, in which firstly a numeric value is assigned to a trust rating for that entity, and a confidence rating is assigned to the estimation of trust. Secondly, the trust and confidence ratings are assigned to fuzzy input sets and processed according to a set of fuzzy rules. Figure 4 shows some exemplary fuzzy input sets. These trapezoidal shapes are simple and convenient forms for the input

15   sets, although the system could of course be implemented using any suitable input set shape, such as those based on Gaussian or sigmoidal distributions.

After fuzzified input variables have been assigned using the sets of figure 4, the resulting outputs are then combined using a matrix of fuzzy rules such as the type indicated in

20   Figures 5 and 6. The system is able to combine any number of Fuzzy Associative Memory (FAM) rule sets for a single authentication process. Alternatively, each individual FAM set might correspond to different context of request (for example, different classes of user such as "accounts", "personnel", "security"). Hence, the system can apply a different set of policy-generated rules to evaluate a user's authentication rating in different contexts.

25

The key benefit in selecting a set of fuzzy rules to produce an authentication response from multiple input sources lies in the ability to apply a set of linguistic operators as IF THEN rules. These allow a smooth mapping of complex policy requirements into automated generation of an authentication decision.

30

The type of Inferencing used in the authentication process is based on numeric processing, i.e. we have a variable number of numeric input elements which need to be integrated to generate a final authenticate response. Future versions of the system could also use more advanced neuro-fuzzy techniques to consider other data sources.

35

In operation a binary Fuzzy Associative Memory system inference procedure activates the antecedent rules of each fuzzy matrix entry to generate the resultant fuzzy output. The illustrations in Figure 5 show example assignment of trust and confidence values to a set of fuzzy rules. In practice a *min* or *max* product rule is used to inference between fired

5   fuzzy rules. To create the output set we can use product inferencing again:

$$\forall x: \mu_{out}(x) = \max(\mu_{out1}(x), \mu_{out2}(x), ...) \qquad \text{Eqn.1}$$

The next stage is to convert the fuzzy output set back into a crisp value. The method
10   chosen in the embodiment is height defuzzification, which is the simplest and fastest method available and ignores both the shape and support of the membership sets, and simply uses the weighted peak of each set. This gives, for the combined fuzzy output set in Figure 5 (bottom right image) a defuzzified authentication rating of 0.42. When this procedure is performed for all possible fuzzy output sets, the resulting outcome is as
15   represented in Figure 6.

In the embodiment, the multiple incoming trust ratings are combined using one FAM set, and the incoming confidence ratings using another. The resulting single trust and confidence ratings are then analysed using a third FAM rule set to obtain the final
20   authentication rating. In Figure 6, therefore, the x-axis represents the FAM input from trust rating assessment, the y-axis represents the FAM input from confidence rating assessment, and the z-axis represents the output authentication rating value.

For alternative embodiments, a wide range of alternative fuzzy operators could be applied
25   with the same effect. This is a common property of Fuzzy Systems and enables the robust and rapid generation of a working rule base to be created.

An advantage of using fuzzy logic as the core inferencing mechanism is that multiple authentication data sets from varied sources can be combined. The system is designed to
30   provide automated software (eg a Web Service as in the embodiment above, or software agents as in the second embodiment below) with the ability to assign an authentication rating to a entity, eg human user, service or external agent. This mechanism is ideally suited to the development of e-commerce and web service processes. Although in the embodiment above, only two sets of authentication data were utilised, this may be
35   increased to any number of different sources.

8

A second embodiment according to the invention will now be described with reference to Figures 7 and 8. Figure 7 is a schematic showing the use of distributed authentication servers 1 within a multi-agent collaborative scenario. In this arrangement, a plurality of

5   agents 71 provide a mechanism for collaborative behaviour which enables interaction and distribution of information between multiple sources, so as to provide a robust authentication mechanism. Each agent 71 is in communication with a local authentication server, and the system operates as follows. Agent 1 might initiate an authentication request based on input from the user 5. The agent broadcasts the request to agents 2

10   and 3 as an XML formatted message, for example see listing 1 below:

```
      <?xml version="1.0" encoding="UTF-8" ?>
      <Authenticate>
      <Principal>agent</Principal>
15    <Category>accounts</Category>
      <TrustValue>0.564</TrustValue>
      <ConfidenceRating>0.99</ConfidenceRating>
      <Policy>D:\trust\policy</Policy>
      <Recommenders>
20            <Agents>
                    <ID>
                    < Fred>
                    </ID>
                    <ID>
25              < Phobos>
                    </ID>
              </Agents>
      </Recommenders>
      </Authenticate>
```

30   **Listing 1. Example XML based Authenticate message object (formatted authentication message that is exchanged between authentication systems or agents).**

Upon receipt of this XML message, Agents 2 and 3 query their local authentication servers, and obtain an authentication response message for the specified user. They

35   return the data to Agent 1 which then combines the returned data with its local assessment of the user's authentication status and passes the data to its local authentication server to generate a final authenticate response for this user. Table 1 below illustrates a set of example trust and confidence ratings output by each of the local authentication servers fuzzy inferencing mechanism:

40

	Agent 1	Agent 2	Agent 3
Trust Rating	0.3	0.6	0.9
Confidence Rating	0.5	0.7	0.8
Authentication Rating	0.4	0.8	0.88
Threshold Response	reject	accept	accept

Table 1: Set of example parameter values (ratings) generated by the three distributed authentication servers in Figure 7, in response to the three agents processing a single user authenticate query.

5   Figure 8 illustrates a modified version of the computer network of Figure 1, adapted to include an agent server 8 in communication with the web server 2 and authentication server 1. In the second embodiment, an example scenario might involve for example a corporate Intranet in which a user 5 needs to access an accounts server at a remote site. The user uses a web browser interface 3 to log into a client web application hosted by

10 web server 2, and provides their credentials which are forwarded to the local agent network. An agent (such as Agent 1 in Figure 7) processes the request and broadcasts a new authenticate request into the agent network. After a predefined number N of agents have replied, the requesting agent passes the set of authenticate responses to a local authentication server to generate the final authenticate response and determine if the

15 users access should be granted.   From the parameters in table 1 above, this authentication might be performed in one of two ways. On the one hand, the local security policy settings may determine that if 2 out of 3 agents validated the user's authentication status, then authentication is automatically granted. Alternatively, the security policy may dicate that all the trust and confidence ratings supplied by the agents must be combined

20 together by the fuzzy inferencing module in the manner similar to that discussed earlier.

    As already discussed, a significant benefit of using fuzzy logic is the ability to combine various heterogeneous sources of data associated with the level of trust for a user. In Figure 9, a block diagram illustrates examples of the various types of inputs which may be

25 used during processing by the inferencing component 25 of the embodiments. Agent inputs 92, such as the type indicated in Table 1 provided in the form of XML formatted messages, are one possible input source. A further input source is data provided by a local case history database 94. Further inputs might include, for example, key evaluations 92, in which another entity (e.g. software agent, authentication server, etc) indicates its

30 acceptance of the authentication of a user by sending its public key.   Finally, any other

sources 93, such as numeric or linguistic assessments of the trust associated with a user, can be combined using an appropriate set of fuzzy rules. All these types of source can be input together to the fuzzy inferencing module 25 for generating an authentication assessment of a particular user (or any other type of entity), the results of which are then

·5   output using an appropriate authenticate message 95 (for example, the XML message object 27 described for Figure 2).

In the embodiments, the exchange of formatted messages allows the exchange between authentication servers of trust / authentication ratings of specific users. In this manner,

10   developed knowledge of a specific user can be exchanged and integrated into the local user databases of multiple authentication systems. This enables a distributed database to be constructed which increases the robustness of the overall authentication service (ie when authentication of a particular user is requested, the necessary data can be retrieved from a number of alternative servers). However, a further aspect of the embodiments is

15   that they also allow policy rules and fuzzy inferencing rules to be exchanged between servers. An example of when this might be used is if a new class of users was added to the system which needed a different authentication profile (e.g. contract staff may require a higher degree of authentication than permanent staff). In this case, a sysstem administrator would only need to add the new policy rules / fuzzy rule set to one of the

20   authentication servers, and they would automatically be propagated across the distributed authentication system by the software agents. An example of an XML message containing an encoded fuzzy rule is given below in Listing 2:

```
      <?xml version="1.0" encoding="UTF-8" ?>
25    <Authenticate>
      <Principal>agent</Principal>
      <Category>accounts</Category>
      <TrustValue>0.564</TrustValue>
      <ConfidenceRating>0.99</ConfidenceRating>
30    <Policy>D:\trust\policy</Policy>
      <Knowledge Base>
              <fuzzyset>
                  <ID>
                  <New Rule from Agent 1>
35                </ID>
                  <fuzzyparameter> 0.3,0.5,0.1,0.6,0.3
                  <fuzzysettype> trapezoid
                  <fuzzysetname> low
              </fuzzyset>
40    </Knowledge Base>
```

</Authenticate>
Listing 2 Example XML Authenticate object containing an encoded fuzzy rule. This message
and rule can be transferred between authentication servers, parsed and the rule inserted into
the receiving rule base.

5

Whilst in the embodiments, the structured message format used to communicate with the authentication server(s) is based on XML, the messages could be appropriately modified to integrate with any particular XML security standard, such as XKMS or SAML (Secure Authentication Markup Language) [http://www.oasis-open.org] for industrial compatibility.

10   Alternatively, any other suitable distributed authentication protocol could be used.

It will be understood by those skilled in the art that the apparatus that embodies the invention could be a general purpose device having software arranged to provide an embodiment of the invention. The device could be a single device or a group of devices

15   and the software could be a single program or a set of programs. Furthermore, any or all of the software used to implement the invention can be contained on various transmission and/or storage mediums such as a floppy disc, CD-ROM, or magnetic tape so that the program can be loaded onto one or more general purpose devices or could be downloaded over a network using a suitable transmission medium.

20